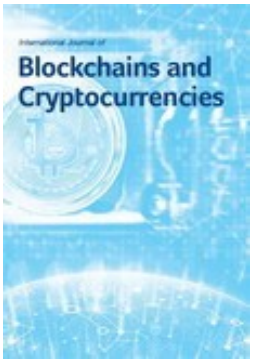
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Blockchains and Cryptocurrencies

ISSN online: 2516-6433 - ISSN print: 2516-6425

https://www.inderscience.com/ijbc

Supply chain provenance with offline verification through a low-requirement, blockchain-based framework

Tabish, Raisa Arief, Auqib Hamid Lone and Roohie Naaz Mir

DOI: 10.1504/IJBC.2022.122988

Article History:

Received:	29 July 2021
Last revised:	29 July 2021
Accepted:	05 December 2021
Published online:	19 May 2022

Supply chain provenance with offline verification through a low-requirement, blockchain-based framework

Tabish, Raisa Arief, Auqib Hamid Lone* and Roohie Naaz Mir

Department of Computer Science and Engineering,
National Institute of Technology,
Srinagar, India
Email: tabish_09btech16@nitsri.net
Email: raisa_03btech16@nitsri.net
Email: ahl@nitsri.net
Email: naaz310@nitsri.net
*Corresponding author

Abstract: Blockchain proves to be an ideal candidate for establishing provenance in supply chains. For ensuring widespread adoption, such frameworks must have low cost-overheads while guaranteeing protection from counterfeiting and must provide end-to-end transparency. A vast majority of existing platforms that attempt to address the lack of provenance knowledge do so by relying on centralised architectures or through the use of high requirement hardware components. In this paper, we propose a robust and adaptable provenance framework running on the decentralised blockchain architecture, along with P2P based offline verification, to address the most common supply chain attacks. Minimal assumptions have been made about the hardware required for enforcing such a platform in general supply chains. The proposed system also allows fully off-chain verification of product attributes and semi-online verification of product ownership using cryptographic methods. This allows a decentralised and cryptographically secure flow of provenance knowledge in supply chains.

Keywords: provenance; supply chain; blockchain; anti-counterfeiting; P2P architecture.

Reference to this paper should be made as follows: Tabish, Arief, R., Lone, A.H. and Mir, R.N. (2022) 'Supply chain provenance with offline verification through a low-requirement, blockchain-based framework', *Int. J. Blockchains and Cryptocurrencies*, Vol. 3, No. 1, pp.41–59.

Biographical notes: Tabish received his BTech in Computer Science and Engineering from the National Institute of Technology, Srinagar, India in 2020. Since 2020, he has been working as a Software Development Engineer at Increff, Bengaluru, India where he is designing cloud-based supply chain management software. His research interests are primarily in designing robust, secure, and scalable automation systems.

Raisa Arief holds a Bachelor's in Computer Science Engineering from the National Institute of Technology, Srinagar. Since 2020, she has been working as a Software Engineer at Eagleview, developing GIS-based microservices. Her research interests include blockchain-based software, scalable architectures, and secure systems.

Auqib Hamid Lone has received his PhD degree from National Institute of Technology, Srinagar, India in 2021. He has completed his MTech in Information Security and Cyber Forensics from Jamia Hamdard University, New Delhi with university rank. He is currently working as a Blockchain Research Scientist at Parfin. His areas of interest are blockchain technology, cryptography, network security, web application security and digital forensics.

Roohie Naaz Mir is a Professor and the Head of Department Computer Science and Engineering at National Institute of Technology Srinagar, India. She received her BE (Hons) in Electrical Engineering from University of Kashmir (India), ME in Computer Science and Engineering from IISc Bangalore (India) and PhD from University of Kashmir, (India). She is a Fellow of IEI, IETE, a senior member of IEEE, member of IACSIT and IAENG. She is the author of many scientific publications in international journals and conferences. Her current research interests include network security, reconfigurable computing, mobile computing, security and routing in networks.

1 Introduction

A remarkable trend being observed in global supply chains is the growing demand for details of the systems and sources that produce and deliver the goods. Every product has a long and storied history. However, much of this history is presently obscured (Francisco, 2018). The existing centralised traceability frameworks in place have considerable risks of data tampering (Dutta et al., 2020). Perceived risks that stem from a lack of such information exert influence on a customer's buying decisions (Kim et al., 2008; Cheney et al., 2009). The growing concerns of consumers and the government regarding food quality have also renewed the concept of traceability in the supply-chain (Shahid et al., 2020). Knowledge of the creation, chain of custody, and modifications of goods in supply chains plays a vital role in alleviating such customer-perceived risks. This information collectively constitutes what is known as provenance knowledge in supply chains (Cheney et al., 2009). Modern supply chains extend across geographies such that, even before reaching the end consumer, goods often travel through a vast network of intermediaries, yet, in almost every case, these journeys remain an unseen dimension of our possessions (Provenance.org, 2015). The traditional supply chains are centralised, and they depend on a third party for trading. These centralised systems lack transparency, accountability, and auditability (Shahid et al., 2020). Often, when negative practices are exposed, they quickly escalate to scandalous and financially crippling proportions. Numerous scandals involving major supply chain producers have come forth due to a lack of public visibility in their manufacturing processes and practices. Worker unrest at Foxconn, one of Apple's major Chinese suppliers, forced the company to pull the curtain back on part of its supply chain in 2009 (New, 2010). Mattel faced a tornado of publicity about lead in toys, which raised questions about how much control the organisation had over its supply chain (New, 2010). Numerous other instances of misconduct in the food, pharmaceutics, electronics, and other supply chains have remained concealed due to insufficient provenance knowledge (Montecchi et al., 2019). Moreover, traditional supply chain systems are not versatile and transparent enough to accommodate the growing needs and demands of the future, leading to substantial

overheads in terms of error handling, costs, administration, and fraud management (Dutta et al., 2020).

Provenance knowledge allows supply chain producers to tackle the crucial problem of counterfeits in national/international trade. Organisation for Economic Co-operation and Development (OECD) estimates that product counterfeiting amounted to roughly US$250 billion of losses in 2007 (Avery, 2008). Counterfeiting is especially prevalent in industries such as fashion, pharmaceuticals, and electronic components. Moreover, the Counterfeiting Intelligence Bureau (CIB) claims that counterfeit goods make up nearly 7% of all world trade (Scorpecci, 2009). End-to-end supply chain transparency and visibility can help model the flow of products from raw materials to manufacturing, testing, and finished goods, enabling new kinds of analytics for operations, risk, and sustainability. Swift identification is critical to minimising negative consequences, and without visibility across a 'system of systems', conducting root cause and impact analyses become labour-intensive and error-prone (Saeed et al., 2013). As supply chains become more global, it has become imperative that organisations maintain accurate provenance knowledge of their items. Blockchain plays a significant role in evolution of supply chain with its inherent properties like decentralisation, transparency and immutability (Shahid et al., 2020). Full transparency is only achieved when all supply chain actors adopt and contribute their data, requiring multiple partners in the supply chain to adopt in order to leverage the network effect (Sternberg et al., 2021).

In this paper, we try to set up the architecture for a provenance platform that enables end-to-end visibility of products flowing in a supply chain, from the producer to the end user. We use the distributed architecture provided by blockchain (Nakamoto, 2008), and introduce decentralisation in our proposed implementation. The principal focus is to maintain visibility at all points within the supply chain while tackling both modification and cloning attacks. We rely on the capabilities and limitations of Ethereum Smart Contracts to ensure the practical viability of all suggested mechanisms (Dannen, 2017). We also attempt to lessen cost overheads and stringent hardware requirements by making minimal presumptions about the kind of hardware to be used for product labelling. Application of electronic tags (NFC or RFID) for product labelling and identification presents appealing security features such as secure memory, read-only storage, and cryptographic capabilities. However, relying on such mechanisms entails the assumption that corresponding security protocols would be strictly enforced. The cost-of-use also builds up considerably when employing sophisticated tags to label individual items. To address this, we try to curtail dependence on such specialised hardware features while maintaining security. Readily available internet connection is not a luxury every customer can afford while merely browsing items. However, knowledge about the product's origins is still an important factor that consumers consider while purchasing a product. We thus make a case for offline verification, which allows product and ownership verification off-chain through the application of digital signatures and P2P data transfer, which can seamlessly be integrated with the existing provenance system.

2 Literature review

Establishing provenance and traceability of items still remains an open problem in the supply chain. Although provenance systems have existed at some level in most supply chains for years, a primary limitation of such systems is their inherently centralised

architecture. This leads to impediments in the traceability of the genuine origins of an item as the system employs centralised authorities due to concerns of tampering. Centralised provenance models delegate the responsibility of maintaining and providing the transaction history from the manufacturer to the centralised provenance provider. This prevents the consumer from obtaining a granular level provenance knowledge of the items. Furthermore, this data can be corrupted and altered. To resolve this, blockchain proves to be an ideal candidate for providing decentralised and immutable provenance knowledge. Blockchain could arguably enable truly sustainable supply chains (Paliwal et al., 2020). It has vast potential to transform the SCs, both global and local, by improving operational efficiency, data management, responsiveness, transparency and smart contract management. With blockchain bursting out on the scene, it can act as a source of competitive advantage for companies, governments and all other kinds of organisations (Dutta et al., 2020).

Consumers are now becoming more aware of the origins of the items they purchase. Missing product details deter a consumer from purchasing an item. Establishing provenance knowledge provides four types of assurances to the customer: Origin, Authenticity, Custody and Integrity assurance (Montecchi et al., 2019).

The various supply chain objectives are cost, quality, speed, dependability, risk reduction, sustainability, and flexibility. Kshetri (2018) examines the likelihood of blockchain achieving these objectives. An evidence-based study is performed linking the use of blockchain to an increase in transparency and accountability across the supply chain system. Due to its decentralised nature where no single company has total control, using blockchain as the underlying technology for supply chain can resolve problems of accountability between individuals and institutions whose interests are not necessarily aligned (Casey and Wong, 2017).

Abeyratne et al. review the current status of blockchain technology for provenance and use the manufacturing of cardboard boxes as an example to theoretically demonstrate how such technology could be used in a global supply chain network (Abeyratne and Monfared, 2016).

The likelihood of the adoption of a blockchain solution for supply chain provenance heavily depends on the ease of integration into the existing established supply chain systems. The benefits only occur if multiple supply chain actors adopt the technology. Improved supply chain transparency, secure information sharing, and operational improvements cannot be achieved solely by individual technology adoption (Sternberg et al., 2021). Sternberg et al. (2021) attribute the reason for few successful implementations of blockchain in supply chain systems to the lack of theoretical and empirical data around it and propose a theory-based model for inter-organisational adoption.

As IoT use has gained traction, it has begun to be used in supply chain systems. An early RFID-based, anti-counterfeiting scheme was proposed by the US FDA (Food and Drug Administration) in 2004. Although this system was vulnerable to tag-cloning attacks, various mechanisms have been proposed ever since to address the same. Yadav et al. (2020) also describe virtual supply chains, which bear the features such as real-time tracking and monitoring of goods flow in the physical supply chain. Their work aims to integrate blockchain with current virtual supply chains, thus eliminating or changing the roles of intermediaries in the virtual supply chain and facilitating transparency, integrity, and authenticity of food supply chain data (Yadav et al., 2020).

Caro et al. (2018) proposed AgriBlockIoT, a multi-layered architecture using blockchain in conjunction with IoT technologies to achieve provenance in the supply chain. This approach provided granular level knowledge about the product, right from the time the seed is planted into the ground (Caro et al., 2018). Yadav et al. also propose utilising RFID tags for food supply chains to provide real-time tracking by storing farm-level information on the tag and updating it with each transaction within the supply chain. However, such approaches rely mainly on IoT devices like sensors to automate the process, procurement of which may not be entirely feasible for businesses. A major shortcoming of using RFID tags is that reading RFID tags require a special RFID reader, which is not readily available to the average consumer.

Saeed et al. resolve the issue of using an RFID tag by replacing it with 2 NFC tags. Since most modern phones have NFC readers in them, a consumer does not need a separate scanner to read the data on the tags. This method employs a tag initiator, which generates a public and private key for each item. It also allows for offline product verification by storing the cryptographic key on one of the tags. This secret key K_s is stored within the tag memory but at a secure location that is only accessible to the tag's processor and, therefore, inaccessible to a reader. Furthermore, the tags are embedded on the item to prevent tag reapplication (Saeed et al., 2013). This method, although secure, is not a viable or cost-effective solution for smaller, less expensive items. The widespread use of electronic tags came with its own set of limitations.

Shahid et al. (2020) introduce a model for the Agri-Food supply chain with an added reputation system. This system is proposed to maintain credibility of the entities of the supply chain and quality ratings of the product. Unlike traditional supply chain systems, the hash of the reviews is stored on the blockchain to ensure immutability and integrity of reviews. The buyer registers their reviews at every transaction in the supply chain, thus ensuring that the credibility of every participant in the supply chain is recorded.

Lehtonen et al. (2008) describe general attack scenarios of illicit actors against product authentication systems through the four categories omission of product's security features, usage of misleading security features on counterfeit products, cloning and imitation of security features, and removal and reapplication of genuine security features. Alzahrani and Bulusu (2018) simplify these attacks into the following classes, which we use primarily in our discussion.

1 *Modification attacks:* Attacks involving the alteration of a product's advertised attributes, such as changing the expiration date.

2 *Cloning attacks:* Attacks involving cloning of a genuine product's attributes for use with a counterfeit product.

3 *Reapplication attacks:* Attacks involving the removal of a legitimate tag from a genuine product and its reapplication to a counterfeit product.

Alzahrani and Bulusu (2018) also propose a decentralised supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC). They use a basic, static TID (tag-ID) assumption to ensure a tag is not modified. However, this tag ID is not always unique, thus making this approach ineffectual.

Toyoda et al. propose a novel product owner management system (POMS) of RFID-attached products for anti-counterfeits that can be used in the post-supply chain. This method addresses the issue of cloning and proves that the cloned tags will be rendered useless if ownership cannot be proved. Thus, an adversary cannot resell a

cloned item as it provides no monetary value to them (Toyoda et al., 2017). Lehtonen et al. 2009 also put forward a method to secure RFID systems by detecting tag cloning using synchronised secrets.

Addressing reapplication attacks largely remains an open problem as the link between a tag and a product is adhesive bonding (Nochta et al., 2006). Signing product-specific features on the label (Nochta et al., 2006) or irrevocably binding an unclonable label to the product can thwart reapplication attacks. However, because acquiring and reapplying authentic labels is expensive and merits no financial gain to the adversary, such an attack does not threaten authentication systems at a large scale (Lehtonen et al., 2008; Toyoda et al., 2017).

3 Limitations of existing schemes

A typical trend in supply chain provenance systems which use electronic identification tags is to rely on the application of hardware-specific tag-features to eliminate tag-cloning. More sophisticated approaches to uniquely identifying electronic-tags in the supply chain include the use of physically unclonable functions (PUFs). PUFs are circuits implemented using different CMOS technologies that act as hardware-fingerprints and are unclonable (Babaei and Schiele, 2019). We argue that, although these implementations ensure defense against the cloning of tags, they have two crucial disadvantages. First, NFC tags are prone to damage as their lifespans are significantly affected by factors like moisture, temperature, abrasion, chemical exposure, UV light, and physical interaction. If by nature, the tag cannot be cloned/replaced without the manufacturer's involvement, it poses a significant hurdle in economically viable, time-sensitive, practical implementations. Secondly, the tag-issuer must assume responsibility for ensuring the use of appropriate types of electronic tags that rigorously adhere to such security standards. In the case of supply chain management, the manufacturers would have to take up the responsibility of issuing the required tags for each product. Once again, this is a challenging constraint to practically enforce across all manufacturers using the platform.

While considering NFC tags for electronic storage, it is pertinent to examine their storage capabilities. Although NFC tags are more convenient to interact with through the use of any NFC compatible smartphone, the average storage capacities of these tags prove to be a considerable blockade. The memory of the most commonly used NFC Type-2 Tags varies between 48 bytes and 8,000 bytes (Smiley, 2020) which happens to be sufficient for storing a URL or a small amount of text. Therefore, such tags can, at best, be utilised for storing rudimentary product attributes and identifiers (Griffiths, 2015). Such limited memory proves to be an obstacle when implementing schemes requiring accommodation of public/private keys, digital signatures, or other comparatively more sizable data on the tag's memory (Alzahrani and Bulusu, 2018; Saeed et al., 2013).

The adoption of blockchain in the supply chain management system can prove highly beneficial for organisations as it helps reduce counterfeit items, thus saving them millions of dollars yearly in addition to improving their reputation. However, the methods proposed cannot be optimally integrated into the existing systems without making significant changes to the existing system. Furthermore, having a continuous internet access is not a luxury every consumer can afford. In the following sections, we propose a

low requirement, provenance method for supply chain traceability using blockchain with an added feature of offline verification of the products origins. We draw inspiration from this POMS system in our approach to addressing blockchain provenance. We aim at building a more adaptable provenance system with offline verification using blockchain technology that adds minimal overhead on the participants in the supply chains while ensuring a high standard of security and assurance.

4 Materials and methods

At an elementary level, a supply chain comprises of producers, consumers, and intermediaries, such as distributors and retailers. The accumulation of provenance knowledge commences with the production of an article by a registered and verified manufacturer. Starting from the manufacture, the account of each transaction involving the product is added to the blockchain. The record of all such transactions, collectively, constitutes the provenance knowledge of a product. At every step in the supply chain, complete knowledge about the origin, chain of custody, authenticity, integrity, as well as subsequent modifications of the product are stored, as part of this provenance knowledge, on the blockchain (Montecchi et al., 2019).

Table 1 Structure of serialised global trade item number (SGTIN) code, which is the EPC schema to encode a GTIN

Header	*Filter value*	*Partition*	*Company prefix*	*Item reference*	*Serial number*
8 bits	3 bits	3 bits	20–40 bits	4-24 bits	38 bits

Note: GTIN identifies a specific group of identical products, while SGTIN identifies each unit of identical products using serial numbers.

Source: GS1 (2017)

Establishing an anti-counterfeiting, provenance platform begins by distinctly identifying producers within the supply chain, as only verified producers should be capable of introducing products to the supply chain. Toyoda et al. (2017) suggest an administrating party, such as GS1, that operates the manual verification and registration of new manufacturers through a dedicated smart contract. The verification process may be automated by delegating the authentication of a manufacturer's identity to a certificate authority (CA). Depending on the operational standards of the issuing authority, different trust models might be employed for validating the applicant's identity. Organisation validation (OV) and extended validation (EV) certificates require a rigorous vetting procedure. Generally, this entails numerous criteria being fulfilled to establish the legal identity, physical presence, and domain control of an organisation (SSLRenewals, 2019). Once the identity is validated, the manufacturer's profile is added to the blockchain by an administrator[1]. A registered profile will contain principal details of the manufacturer, such as brand name, location, and domain. Each manufacturer profile stores a unique company-prefix as well which is attached to each product, along with the product's identifying serial number. The company-prefix enables the mapping of a product to its corresponding producer. Electronic product codes (EPCs), used for product tagging and identification, contain such a company-prefix, assigned to the company by GS1. If not using EPCs, a prefix could be generated manually through the smart contract and

prepended to the product serial number. In the paper, we use the term EPC generally for referring to any such product identifier.

4.1 Proposed provenance framework

In the following sections, we attempt to establish a provenance platform through blockchain and basic cryptography to afford a low cost, low requirement, supply chain traceability system with offline verification. To achieve this, we minimise assumptions regarding the capabilities and type of tags used to identify the products. Further, the proposed scheme exhibits a greater extent of robustness as a result of not relying on potentially damage-prone hardware.

4.1.1 Architecture

Toyoda et al. (2017) proposed a detailed approach for establishing a novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain that partly serves as the base of our provenance system. The approach for implementation is assumed to be through Ethereum smart contracts, written in solidity. A synopsis of the process that establishes provenance knowledge and enforces anti-counterfeiting measures is as follows[2].

1 Product manufacture

   A producer manufactures an item and calls a *produceItem*( ) method on the contract, passing as arguments the product attributes to store on the blockchain. These attributes could include the EPC, price, manufacture date, expiry date, origin, and other relevant product information. Since retrieval of product attributes is done based on the EPC, product attributes are stored on-chain as an EPC-to-attributes mapping. Additionally, the blockchain must enforce three necessary constraints at this step – first, the caller of *produceItem*( ) must be a registered manufacturer, second, the company-prefix within the EPC must be identical to the company-prefix assigned to the caller, and third, any other product with the same EPC should not have been produced previously.

2 Shipment and change in ownership

   Once the product is manufactured, the smart contract assigns the manufacturer's Ethereum-address to a 'currentOwner' variable, corresponding to the product. To initiate a transaction for changing ownership, a *shipProduct*( ) method is invoked by the current owner, passing the receiver's Ethereum-address as an argument. Calling *shipProduct*( ) sets the *state* of the product to '*shipped*' and stores the recipient's address on the blockchain. The receiver must invoke a *receiveProduct*( ) method, to gain ownership once the item is physically received. If this call is successful, the ownership changes on the blockchain, and the *status* is reset. The constraints for calling *shipProduct* are that the caller must be the current owner and that the status must not be '*shipped*'. The constraints for calling *receiveProduct*( ) are that the recipient's Ethereum address matches the one specified by the initiator of the shipment and that the product status is '*shipped*' (Toyoda et al., 2017).

3 Logging transactions

At any step throughout the product's journey where a meaningful change occurs in the state, an event is fired to signify the said change. In Ethereum, 'events' are dispatched signals that the smart contract can fire to immutably log a transaction occurring on the blockchain. Such events may identify the item's production, shipment initiation and shipment receipt, among other events.

4 Product verification

At any point, the provenance knowledge of a product might be retrieved from the blockchain by invoking a *getProduct*( ) method, passing the EPC as an argument. More specifically, before purchasing a product or receiving a shipped item, the customer may desire origin, authenticity, custody, and integrity assurances (Solidity Docs, 2016). The collection of events acts as an audit trail providing traceability, certifiability, and verifiability of product information along the supply chain.

4.2 Offline verification scheme

Although online verification of a product is straightforward in a blockchain provenance system, the vast majority of such schemes lack the possibility of performing validation offline as all product data is stored on the chain. Alzahrani and Bulusu (2018) proposed an offline, local authentication scheme that uses digital signatures and public-key cryptography to validate a product off-chain. However, the mechanism of public-key distribution is not discussed which restricts the offline nature of the system. We propose an alternate, cryptographically secure procedure for offline verification that allows a customer to verify the integrity of a product's origin and claimed attributes without being online. To accomplish this, we rely on digital signatures generated from the product attributes and signed by the manufacturer. The product attributes presented to a customer may be compared with this signature to detect any malicious modification performed by an adversary. It is important to note that to carry out a transaction involving a change in the product state, connectivity to the blockchain is mandatory. We use this aspect to augment our offline verification scheme and introduce offline custody verification through a semi-online system.

4.2.1 Offline product attributes validation process

1 The manufacturer (M) specifies the product attributes (D) at the time of manufacture. These details include branding information, pricing data, manufacture and expiry dates, etc.

2 The Manufacturer encrypts the hash digest of product attributes, $hash(D)$, using their Private-Key (Pr_M), to generate the Manufacturer's Product Signature (S_1).

$$S_1 = encrypt\left(Pr_M, hash(D)\right), \tag{1}$$

3 The product signature, S_1, as well as the product details, D, are passed on to the smart contract at the time of registering a new product. The contract verifies the validity of S_1 by using the Manufacturer's Public-Key (Pu_M). If verified, the contract signs the product signature with a contract specific Private-Key, Pr_C, which is

exclusively owned by an administrator. A crucial aspect to note at this point is that, in contrast to externally owned accounts (EOA), contracts accounts do not possess a private key for encryption. Therefore, performing digital signatures directly on the smart contract is not feasible[3]. As a workaround, the responsibility of carrying out this encryption, on behalf of the contract, could be delegated to an encryption server that can securely store and use Pr_C. The result of this second level of encryption generates the Contract's Product Signature, S_2

$$S_2 = encrypt\left(Pr_C, S_1\right), \tag{2}$$

4 Once S_2 is generated, it is returned to the Manufacturer who can validate it using the contract's Public-Key, Pu_C. This 2-step encryption is required to prevent an adversary from providing spurious signatures and keys to a customer (in case only Pr_M is used for encryption), as well as, to prevent centralisation of the system (in case only Pr_C is used for encryption). It is assumed that every user of the platform has a valid copy of Pu_C stored locally on their devices which was obtained at the time of registering for the provenance platform.

5 The manufacturer stores D on a regular barcode, QR Code or an electronic NFC tag which is attached to the product. An auditing party, P, that wishes to survey the details of the product can scan the attached tag and retrieve the product attributes as plaintext.

6 If P desires to authenticate the details claimed on the product, they can request the current owner to provide the signature S_2 as well as the manufacturer's public-key, Pu_M. At the outset, this data is transmitted, from the Manufacturer to party P, over a local network using Bluetooth, WiFi, or any other offline mode of transmission.

7 Once P has access to D (read from the product's tag), S_2 and Pu_M (received locally from the Manufacturer), the auditor can perform the following sequence of steps to complete the verification:

a *Decrypting contract's digital signature:* Using the contract's public key, Pu_C, which is made available locally to all registered users, S_2 can be decrypted

$$S_1' = decrypt\left(Pu_C, S_2\right), \tag{3}$$

b *Decrypting manufacturer's digital signature:* Using the manufacturer's public-key, Pu_M, which was sent locally by the current owner, S_1' may be decrypted to obtain $hash(D')$

$$hash(D') = decrypt\left(Pu_M, S_1'\right), \tag{4}$$

c *Compare the product attributes:*

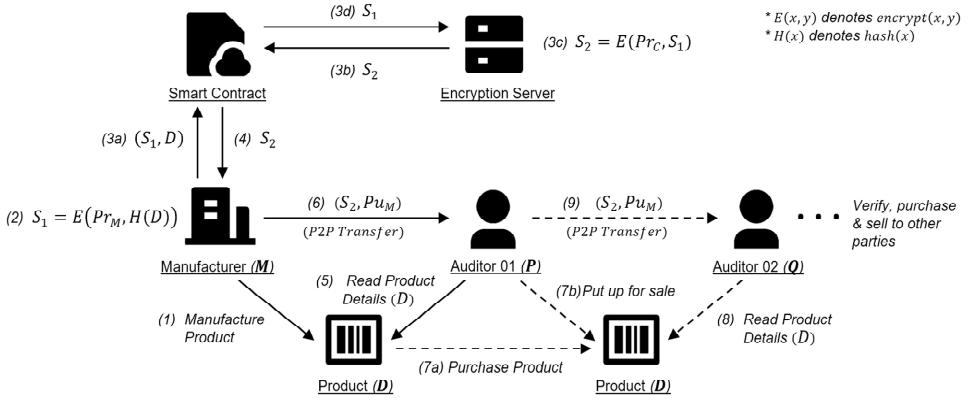
$$hash(D') == hash(D), \tag{5}$$

The comparison performed in the final step reveals whether or not the claimed product attributes match the product attributes set during manufacture of the product. Additionally, after the local transfer of S_2 and Pu_M, the auditing party, P, now has a copy of all the data required to allow local verification of the products attributes. If P decides to purchase and then transfer the product to some party, Q, they can locally transmit the signatures and public-keys to Q. This enables Q to locally authenticate the product. In

this manner, the Manufacturer's Public-Key is passed on to the next owner in a P2P fashion, entirely offline. Such a mechanism also affords the possibility of a seller providing additional product data, e.g., images, links, webpages, etc., to a client, through P2P transfer (see Appendix A).

There could be the argument to instead store signature data on electronic tags, such as NFC or RFID chips, which are readable by end-users. However, as discussed earlier, the storage capabilities of common NFC tags are of the order of a few hundred bytes. In contrast, the storage requirement for public key certificates (for storing Pu_M) and the ECDSA signatures (S_2) is easily over several kilobytes (Alzahrani and Bulusu, 2018; Johnson et al., 2001). Although certain RFID tags provide sufficiently large storage capacities, they also require the use of specialised RFID readers for interacting with them. Such devices might not be at the ready disposal of most end-customers.

Figure 1 Workflow involved in offline product verification scheme



4.2.2 Custody validation using a semi-online mechanism

The offline verification setup discussed in the last section focuses on validating just the product attributes. A semi-online scheme can be established to authenticate the current custodian of the product by leveraging the fact that all transactions must occur on-chain. To set up this scheme, the contract's digital signature, S_2, is updated each time there is a transaction to include some identifier of the genuine current owner. The additional steps to be carried out for this are:

1 When the ownership of a product changes, S_2 is renewed via the contract by digitally signing the Public-Key of the current owner, appended to the Manufacturer's Digital Signature.

$$S_2 = encrypt\left(Pr_C, S_1 + Pu_O\right), \tag{6}$$

where Pu_O is the genuine current owner's Public-Key. This augmented signature, S_2, is updated each time the ownership is transferred by using the latest value of Pu_O. Further, since for a change-of-hands to occur the recipient must be online, the updated value of S_2 is returned as part of the *receiveProduct*( ) call. This allows the current owner to locally store the updated signature in order to allow local verification by an interested customer.

2 An auditing party, interested in validating the product and its ownership, requests the product's custodian for S_2 and Pu_M. Additionally, the auditor requests for two more values (K, N), where N is a random nonce and K is an encryption performed on the same nonce using the custodian's private-key, Pr_O'

$$K = encrypt\left(Pr_{O'}, N\right), \tag{7}$$

3 To verify the custodian's claim of ownership, the auditor decrypts the extended signature to retrieve S_1' (to be used for verifying product details, as discussed previously) and Pu_O, the Public-Key of the genuine current owner, as stored on the blockchain. To verify the custodian's claim of ownership, the following validation should be successful

$$N == decrypt\left(Pu_O, K\right), \tag{8}$$

This scheme has the obvious drawback that a former owner might also claim ownership of a product by using an outdated signature attached to a counterfeit version of the product. However, such conflicts will nevertheless be resolved by verifying the when the potential recipient victim invokes the *receiveProduct*( ) method, and hence, such a claim has little merit for any party.

5 Resilience towards attacks

Considering the three forms of attacks examined previously, we can evaluate how the proposed system fares when facing each form of attack:

1 *Modification attacks*: For performing verification online, the product details are retrieved directly from the blockchain. Since blockchain records are immutable, there is no scope of modification for on-chain data. For offline verification, the 2-level encrypted signature of the product data can be used for verifying claimed product attributes, hence, preventing modification attacks.

2 *Cloning attacks*: By virtue of the logic used in the smart contracts, the only party that can carry out a transaction on a product is the current owner, identified by their Ethereum addresses. Therefore, even if a tag is cloned by an adversary, further transactions on that product cannot be carried out without also forging the Ethereum Addresses of the current owner, which is assumed to be impractical. The semi-online validation process also prevents an attacker from falsely claiming product ownership.

3 *Reapplication attacks*: As previously mentioned, since the link between a product and its tag is of a physical nature, the only practically realisable approach to mitigate such attacks is the embedding of an unclonable tag into the product itself.

5.1 Durability and adaptability of the proposed system

The system proposed so far makes minimal assumptions about the tagging technique used for the product. As such, the entire process can run on top of an NFC/RFID based tagging system, as well as on a printed, QR/Bar-code based tagging system. The proposed approach guarantees a satisfactory level of security, on top of which, the Manufacturer

may add additional features provided by more sophisticated electronic tags, as per their requirement. For instance, instead of relying on P2P data transfer for offline verification, more expensive electronic tags with greater storage capacities might be used. Static tag-IDs, as seen in the system proposed by Alzahrani and Bulusu (2018), could be incorporated with the existing signature process if desired by the manufacturer. Cryptographic capabilities of tags and other hardware-specific features can be comfortably accommodated with the proposed scheme to provide the desired level of security.

In terms of resilience, since there is no reliance on hardware-specific features like TIDs, PUFs, etc., the system depicts higher fault tolerance. All the data attached to a product is tamper-proof and can be made publicly visible. Thus, in case of loss of tag-data, recovery can be performed by simply copying the data for a specific product from the blockchain to a fresh product tag without involving the manufacturer or administrator. Furthermore, to reduce the problem of data explosion, a collaborative approach of 'on chain and off chain' management of data can be utilised so that a single node is not overloaded with data (Dutta et al., 2020). Security remains un-compromised as the constraints placed on carrying out transactions via the blockchain contracts ensure that only the genuine owner can sell a product and only an authentic recipient may receive a shipped product.

6 Application scenario

An example scenario demonstrating the usage of the proposed system is explained. For this example, the proposed provenance platform is considered for managing the lifecycle of a leather handbag in its supply chain. We focus on the events that occur from the very beginning, starting from the verification and registration of the manufacturer and ending with a consumer purchasing and owning the item. Since the transfer of signature data required for offline verification can be done either through a P2P-based transfer or using sufficiently capable electronic tags, for the sake of simplicity, we assume the use of electronic RFID tags in the use case.

1 *Verification of manufacturer:* A leather handbag manufacturer, who wishes to employ the provenance platform, firstly proves their identity through organisation validation (OV) or extended validation (EV) certificates.

2 *Registration of manufacture:* Once verified, the handbag manufacturer would be added to the system as an administrating user, after which they deploy the smart contract to manage their supply chain. On registration, the handbag manufacturer is also assigned a unique company-prefix which allows validating the ownership of each product since product EPC values must begin with the corresponding company-prefix.

3 *Product manufacture:* The manufacturer produces a leather handbag and invokes a product creation function on the blockchain by passing attributes of the created products, such as its EPC, price, manufacture date, expiry date, origin, and other relevant information. By design, the method invoker's Ethereum address is used to ensure that the genuine handbag manufacturer is indeed requesting the creation of a new leather handbag on the blockchain.

4 *Generation and storing of signatures:* For offline verification, the manufacturer receives the Contract's Product Signature after successful product creation and stores this information on an RFID tag attached to the handbag.

5 *Shipping to transporter:* To transfer ownership of the handbag to the transporter, the producer invokes a product shipping function by specifying the Ethereum address of the transporter as well as the product's identifier.

6 *Verification by transporter:* Before receiving the product, the transporter might want to validate the genuineness of the handbag. This validation can be achieved in a couple of ways.
   a *Online verification of product genuineness:* The transporter obtains the track of all transactions associated with the handbag, as well as its attributes and ownership details, from the blockchain directly. Using this information, they are able to verify the product's genuineness.
   b *Offline verification:* The transporter scans the product signatures present on the attached RFID tag and locally performs the signature decryption and comparison to the verify authenticity of claimed product attributes and ownership. The Manufacturer's public key is requested locally and transmitted to the transporter over Bluetooth or WiFi.

7 *Confirmation of transfer:* To acknowledge ownership, the transporter will invoke a separate function by providing the product identifier as well. This will ensure that the transporter only receives an item once they are ready to do so. If using the semi-offline custody validation scheme, following the *receiveProduct*( ) method invocation, the signature on the handbag's RFID tag will be updated to reflect the updated ownership.

8 *Further transfer of ownership:* Once the transporter becomes the current owner of the handbag, they are granted authority to transfer the ownership to another party using the same process as discussed in step 5. In case the transporter, or any other current owner, tampers with the claimed product attributes, the validation performed by an interested party would fail. In this manner, the product ownership would be transferred to subsequent parties, finally ending up with the customer who purchases the handbag from a retailer.

9 *Restoring signature data:* In case the RFID tag attached to the handbag that contains the product signatures is lost by the transporter, they can re-fetch the product signatures for that product from the blockchain and store it on a fresh tag. Since the system does not rely on hardcoded, unclonable features of product-tags, restoring tag information is secure and convenient.

7 Conclusions

As organisations are beginning to devote more resources to consumer satisfaction by improving provenance knowledge, the proposed system has immense potential in being used as a backbone for numerous supply chain systems. The core idea of the paper is to establish a blockchain based supply chain system with low requirements so as to seamlessly integrate into the existing systems without any overhead. Given the

non-intrusive nature of the proposed system, current supply chains can be upgraded to the proposed system without significant, if any, disruption.

In addition to proposing a blockchain provenance system, the paper highlights the three major attacks on supply chain. It discusses how they can be overcome through the use of the proposed provenance platform. Furthermore, the paper proposes a method for offline verification of product tags using digital signatures, which are sent using P2P via Bluetooth, Wi-Fi, etc.

Implementation of the said system allows us to achieve other desired objectives such as improvement of transparency, detection and recall of defective items, and eliminate counterfeits in the supply chain.

Use of the smart contracts ensures that each transaction in the supply-chain occurs between authorised and genuine parties. Since there is now greater accountability for each participant at each step, the items are less likely to be intercepted or forged by adversaries.

8 Challenges and future work

Some open problems are present in our approach which require further investigation. Firstly, the reliance on an administrating party for the registration of manufacturers introduces an element of centralisation to the platform. Due to the inability of Smart Contracts to perform encryption, the reliance on a central encryption authority is raised further when using offline verification. The design of a completely software enabled, decentralised, offline verification scheme remains an open area of research.

Secondly, reapplication attacks are assumed to provide no monetary benefit to the adversary since only one version of the product can be sold. However, if the adversary happens to be a registered manufacturer, they would be capable of selling both the genuine and counterfeit versions of the product, one version under the genuine manufacturer's name and the other under their own name. Such an attack vector remains a slightly improbable yet unaddressed security challenge for provenance platforms. Although the intruder may not be able to derive significant monetary value from the forged item, such an attack nevertheless introduces a counterfeit in the supply chain without detection and is thus an open point for future research.

Furthermore, the operational cost of the system could become significantly inflated due to high transaction fees. Toyoda et al. analyse the cost of transactions in a similar system which revealed that the total cost for six transfers is less than US$1 (Toyoda et al., 2017). Therefore, using the existing Ethereum architecture, the system might only be economically viable for relatively expensive products selling at more than US$100 (Toyoda et al., 2017). To make the proposed provenance system feasible for products with lower price ranges, alternate systems might need to be researched. Smart contracts built using technologies with lower transactional fees such as IOTA or even using the upcoming Eth2 (Ethereum 2) upgrade could drive down the transaction fees to more reasonable levels.

Finally, the main advantage that the system provides is transparency. However, the success of this system depends heavily, if not entirely on the organisations openness and willingness to adopt the system. Since this system provides every participant the same level of transparency, it may prove counterproductive to organisations who wish to conceal fine details of their supply chains from their competitors.

References

Abeyratne, S. and Monfared, R. (2016) 'Ledger, blockchain ready manufacturing supply chain using distributed', *International Journal of Research in Engineering and Technology*, Vol. 5, No. 9, pp.1–10.

Alzahrani, N. and Bulusu, N. (2018) *Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain*, pp.30–35, 6pp, Association for Computing Machinery, New York, NY, USA, ISBN: 9781450358385, https://doi.org/10.1145/3211933.3211939.

Avery, P. (2008) *The Economic Impact of Counterfeiting and Piracy* [online] https://www.loc.gov/item/2008456864 (accessed 12 December 2020).

Babaei, A. and Schiele, G. (2019) 'Physical unclonable functions in the internet of things: state of the art and open challenges', *Sensors*, 21 July, Vol. 19, No. 14, p.3208.

Caro, M.P., Ali, M.S., Vecchio, M. and Giaffreda, R. (2018) 'Blockchain-based traceability in agri-food supply chain management: a practical implementation', in *IoT Vertical and Topical Summit on Agriculture – Tuscany*, Tuscany.

Casey, M.J. and Wong, P. (2017) 'Global supply chains are about to get better, thanks to blockchain', *Harvard Business Review*, 13 March [online] https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain (accessed 13 March 2021).

Cheney, J., Chong, S., Foster, N., Seltzer, M. and Vansummeren, S. (2009) 'Provenance: a future history', in *Proceedings of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications*.

Dannen, C. (2017) *Introducing Ethereum and Solidity*, Springer, Berkeley, CA.

Dutta, P., Choi, T-M., Somani, S. and Butala, R. (2020) 'Blockchain technology in supply chain operations: applications, challenges and research opportunities', *Transportation Research Part E: Logistics and Transportation Review*, Vol. 142, Part E, p.102067.

Francisco, K.A.S.R. (2018) 'The supply chain has no clothes: technology adoption of blockchain for supply chain transparency', *Logistics*, Vol. 2, pp.1–13.

Griffiths, D. (2015) *NFC Storage: There's Plenty of Room at the Bottom – Black Pepper Software*, 20 October [online] https://www.blackpepper.co.uk/blog/theres-plenty-of-room-at-the-bottom-nfc (accessed 12 December 2020).

GS1 (2017) *EPC Tag Data Standard*, 1 September [online] https://www.gs1.org/sites/default/files/docs/epc/GS1_EPC_TDS_i1_11.pdf (accessed 12 December 2020).

Johnson, D., Menezes, A. and Vanstone, S. (2001) 'The elliptic curve digital signature algorithm (ECDSA)', *Int. J. Inf. Sec.*, Vol. 1, No. 8, pp.36–63.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008) 'A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents', *Decision Support Systems*, Vol. 44, No. 2, pp.544–564.

Kshetri, N. (2018) 'Blockchain's roles in meeting key supply chain management objectives', *International Journal of Information Management*, pp.80–89.

Lehtonen, M., Ostojic, D., Ilic, A. and Michahelles, F. (2009) 'Securing RFID systems by detecting tag cloning', in *Pervasive Computing, 7th International Conference*, Nara, Japan.

Lehtonen, M., Staake, T., Michahelles, F. and Fleisch, E. (2008) 'From identification to authentication – a review of RFID product authentication techniques', *Networked RFID Systems and Lightweight Cryptography*, 1st ed., Vol. 1, pp.169–187 [online] https://link.springer.com/book/10.1007/978-3-540-71641-9#about

Montecchi, M., Plangger, K. and Etter, M. (2019) 'It's real, trust me! Establishing supply chain provenance using blockchain', *Business Horizons*, Vol. 62, No. 3, pp.283–293.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] https://bitcoin.org/bitcoin.pdf (accessed 13 December 2020).

New, S. (2010) 'The transparent supply chain', *Harvard Business Review*, October [online] https://hbr.org/2010/10/the-transparent-supply-chain (accessed 13 December 2020).

Nochta, Z., Staake, T. and Fleisch, E. (2006) 'Product specific security features based on RFID technology', in *International Symposium on Applications and the Internet Workshops*, Phoenix, AZ.

Paliwal, V., Chandra, S. and Sharma, S. (2020) 'Blockchain technology for sustainable supply chain management: a systematic literature review and a classification framework', *Sustainability*, Vol. 12, No. 18, pp.1–39.

Provenance.org (2015) *Blockchain: The Solution for Transparency in Product Supply Chains*, 21 September [online] https://www.provenance.org/whitepaper (accessed 13 December 2020).

Saeed, M., Bilal, Z. and Walter, C. (2013) 'An NFC based consumer-level counterfeit detection framework', in *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*.

Scorpecci, D. (2009) 'The economic impact of counterfeiting and piracy', in *Presentation at the Conference 'Transatlantic IP Collaboration'*, Washington, DC.

Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F.A., Zuair, M. and Alam, M. (2020) 'Blockchain-based agri-food supply chain: a complete solution', *IEEE Access*, Vol. 8, pp.69230–69243.

Smiley, S. (2020) *atlasRFIDstore*, 7 January [online] https://www.atlasrfidstore.com/rfid-insider/nfc-facts (accessed 12 December 2020).

Solidity Docs (2016) *Contracts — Solidity 0.7.6 Documentation* [online] https://docs.soliditylang.org/en/latest/contracts.html#events (accessed 12 December 2020).

SSLRenewals (2019) *Organization Validated (OV): SSLRenewals*, 6 December [online] https://help.sslrenewals.com/support/solutions/articles/22000218716-organization-validated-ov- (accessed 12 December 2020).

Sternberg, H.S., Hofmann, E. and Roeck, D. (2021) 'The struggle is real: insights from a supply chain blockchain case', *Journal of Business Logistics*, March, pp.71–87.

Toyoda, K., Mathiopoulos, P.T., Sasase, I. and Ohtsuki, T. (2017) 'A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain', *IEEE Access*, Vol. 5, pp.17465–17477, DOI: 10.1109/ACCESS.2017.2720760.

U.S. Department of Health and Human Services (2004) *Combating Counterfeit Drugs*, a Report of the Food and Drug Administration, February [online] http://www.fda.gov/downloads/Drugs/DrugSafety/UCM169880.pdf (accessed 13 December 2020).

Yadav, J., Misra, M. and Goundar, S. (2020) 'An overview of food supply chain virtualization and granular traceability using blockchain technology', *International Journal of Blockchains and Cryptocurrencies*, Vol. 1, No. 2, pp.154–178.

Notes

1 An Administrator, in our discussion, refers to the party that deploys and owns the smart-contracts to establish the proposed Provenance system.

2 It is assumed that the registration of manufacturers, after due verification, has already been performed by an administrator.

3 In theory, it is possible to generate a private key for the contract and use it for encryption, however, any encryption events involving such a key would be publicly visible on account of the transparent nature of the blockchain.

Appendix

Appendix A: Pseudocode for offline product verification (see online version for colours)

```
def manufacture_product():
    product_attributes = b'id:1342; price:USD 120;'
    mfg_product_sign =
        sign_with_rsa(product_attributes, MFG_PVT_KEY, MFG_MOD)

    return product_attributes, mfg_product_sign

def save_details_to_contract(product_attributes, mfg_product_sign):
    assert rsa_verify_signature(
        mfg_product_sign, product_attributes,
        MFG_PUB_KEY, MFG_MOD)

    contract_product_sign = rsa_encrypt(
        mfg_product_sign,
        CONTRACT_PVT_KEY,
        CONTRACT_MOD)

    return contract_product_sign

def verify_contract_signature(contract_product_sign, mfg_product_sign):
    assert
        rsa_decrypt(
            contract_product_sign,
            CONTRACT_PUB_KEY,
            CONTRACT_MOD) ==
        get_bytes(mfg_product_sign)

def verify_product_attributes(contract_product_sign, manufacturer_pub_key):
    product_attributes_to_check = b'id:1342; price:USD 120;'
    calculated_manufacturer_signature =
        rsa_decrypt(
            contract_product_sign,
            CONTRACT_PUB_KEY,
            CONTRACT_MOD)
```

Appendix A: Pseudocode for offline product verification (continued) (see online version for colours)

```
    assert rsa_verify_signature(
            get_int(calculated_manufacturer_signature),
            product_attributes_to_check,
            manufacturer_pub_key, MFG_MOD)


def main():
    # 1. Manufacturer specifies product attributes and
    # a mfg_product_sign on product manufacture
    product_attributes, mfg_product_sign = manufacture_product()

    # 2. Manufacturer requests upload of product
    # details to the blockchain.The contract verifies the mfg_product_sign
    # and, if validated, generates a contract_product_sign
    contract_product_sign =
        save_details_to_contract(product_attributes, mfg_product_sign)

    # 3. Manufacturer validates the contract_product_sign.
    # If validated, the manufacturer passes on the product attributes,
    # contract_product_sign an manufacturer's public key to the next owner
    verify_contract_signature(
        contract_product_sign,
        mfg_product_sign)

    # 4. Either add product attributes, signatures & manufacturer public key
    # to a tag, physically attached to the product OR transfer via P2P

    # 5. An auditing party who wants to verify the product
    # details must collect the contract_product_sign and
    # manufacturer product key from the previous owner.
    # Using this data, they can validate the details attached to the product
    verify_product_attributes(contract_product_sign, MFG_PUB_KEY)
```